

RECEIVED
CENTRAL FAX CENTER

JAN 19 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Lotspiech)	Art Unit: 2134
)	
Serial No.: 10/042,652)	Examiner: Berger
)	
Filed: January 8, 2002)	ARC920010090US1
)	
For: METHOD FOR ENSURING CONTENT)	January 19, 2006
PROTECTION AND SUBSCRIPTION)	750 B STREET, Suite 3120
COMPLIANCE)	San Diego, CA 92101
)	

APPEAL BRIEF

Commissioner of Patents and Trademarks

Dear Sir:

This brief is submitted under 35 U.S.C. §134 and is in accordance with 37 C.F.R. Parts 1, 5, 10, 11, and 41, effective September 13, 2004 and published at 69 Fed. Reg. 155 (August 2004). This brief is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

<u>Section</u>	<u>Title</u>	<u>Page</u>
(1)	Real Party in Interest.....	2
(2)	Related Appeals/Interferences.....	2
(3)	Status of Claims.....	2
(4)	Status of Amendments.....	2
(5)	Summary of Claimed Subject Matter	2
(6)	Grounds of Rejection to be Reviewed.....	4
(7)	Argument.....	5
App.A	Appealed Claims	
App.B	Evidence Appendix	
App.C	Related Proceedings Appendix	
		01/23/2006 BABRAHA1 00000022 090441 10042652
		02 FC:1402 500.00 DA

1053-130.44P

BEST AVAILABLE COPY

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 2

PATENT
Filed: January 8, 2002

(1) Real Party in Interest

The real party in interest is IBM Corp.

(2) Related Appeals/Interferences

No other appeals or interferences exist which relate to the present application or appeal.

(3) Status of Claims

Claims 1, 3-25, and 28-48 are pending and finally rejected, and Claims 2, 26, and 27 are canceled. It is believed that because the only rejections of Claims 17-22 were based on a double patenting rejection that has since been removed by the filing of a terminal disclaimer, only the rejections of Claims 1, 3-16, and 23-25, and 28-48 are being appealed herein.

(4) Status of Amendments

No amendments are outstanding.

(5) Summary of Claimed Subject Matter

As an initial matter, it is noted that according to the Patent Office, the concise explanations under this section are for Board convenience, and do not supersede what the claims actually state, 69 Fed. Reg. 155 (August 2004), see page 49976. Accordingly, nothing in this Section should be construed as an estoppel that limits the actual claim language.

1053-130.A.PP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 3

PATENT
Filed: January 8, 2002

Claim 1 recites a method for securely transmitting multicast data that includes encrypting at least one title T with at least title key K_T (block 26, figure 3; page 12, lines 3-19) and encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S (block 28, id.) to render a multicast data channel encrypted as $S_{K_{cu}}(K_T)$, $S_{K_T}(T)$, wherein the channel-unique key K_{cu} is the result of a combination of a channel key K_c and a session key K_s , id.

Claim 24 sets forth a method for enforcing copy protection compliance and subscription compliance that includes providing players with respective device keys K_d useful for enabling copy protection compliance (block 18, figure 2; page 11, lines 9-16), and providing players with at least one channel key K_c useful for enabling subscription compliance (block 20, id.), such that a player can decrypt content only if the player is both compliant with copy protection and the player is an active subscriber to a content channel. The method also includes encrypting at least one title T with at least title key K_T , supra, and encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{K_{cu}}(K_T)$, $S_{K_T}(T)$, wherein the channel-unique key K_{cu} is the result of a combination of the channel key K_c and a session key K_s , supra.

Claim 41 requires a player (12, figure 1; page 9, line 17) for decrypting streamed content that has at least one device key K_d , supra, means (processor discussed on page 10, lines 12-15) for decrypting a session key K_s using the device key K_d , and means for decrypting a channel unique key K_{cu} using at least the session key K_s . Means are provided for deriving a title key K_T using at least the channel unique key K_{cu} , with the title key K_T being useful for decrypting content.

Claim 44 sets for a computer program device that has a computer program storage device including a program of instructions usable by a computer, e.g., player 12 with processor and software, supra. The

CASE NO.: ARCY20010090US1
Serial No.: 10/042,652
January 19, 2006
Page 4

PATENT
Filed: January 8, 2002

device includes logic means for receiving private information I_u upon registration with a content provider, block 18, supra, and logic means for subscribing to at least one content channel provided by the content provider, supra. Also, the device includes logic means for receiving at least one encrypted channel key K_e at least partially in response to subscribing to the channel. Logic means derive the channel key K_e using the information I_u , and logic means use at least the channel key K_e to decrypt content streamed over the channel.

(6) Grounds of Rejection to be Reviewed on Appeal

- (a) Claims 41-46 have been rejected under 35 U.S.C. §102 as being anticipated by Richards, USPN 6,690,795.
- (b) Claim 1 has been rejected under 35 U.S.C. §103 as being unpatentable over Yokota et al., USPN 6,691,149 in view of Ishiguro et al., USPP 2002/0083319.
- (c) Claim 1 has been rejected under 35 U.S.C. §103 as being unpatentable over Knauft, USPP 2001/0029581 in view of Ishiguro et al.
- (d) Claim 1 has been rejected under 35 U.S.C. §103 as being unpatentable over Richards in view of Ishiguro et al.
- (e) Claims 3-16, 23, and 47 have been rejected under 35 U.S.C. §103 as being unpatentable over Yokota in view of Ishiguro.
- (f) Claims 3-16, 23, and 47 have been rejected under 35 U.S.C. §103 as being unpatentable over Knauft in view of Ishiguro.
- (g) Claims 3-16, 23-25, 28-40, 47, and 48 have been rejected under 35 U.S.C. §103 as being unpatentable over Richards in view of Ishiguro.

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 5

PATENT
Filed: January 8, 2002

(7) Argument

As an initial matter, it is noted that according to the Patent Office, a new ground of rejection in an examiner's answer should be "rare", and should be levied only in response to such things as newly presented arguments by Applicant or to address a claim that the examiner previously failed to address, 69 Fed. Reg. 155 (August 2004), see, e.g., pages 49963 and 49980. Furthermore, a new ground of rejection must be approved by the Technology Center Director or designee and in any case must come accompanied with the initials of the conferees of the appeal conference, *id.*, page 49979.

Appellant notes that the SPE signed off on the final rejections. Accordingly it is not expected that reopening of prosecution will occur, since the SPE has already had the chance to consider the gravamen of the arguments below and has rejected them.

(a) First considering Claim 41, the program key Pk of Richards, figure 14 embodiment, has been relied on as the claimed title key "useful for decrypting content." However, the program key Pk of Richards is useless for decrypting content, because it is used to derive the segment key Sk - the only thing in the relied-upon embodiment of Richards that is "useful for decrypting content", col. 11, lines 21 and 22. The rejections merit reversal.

Additionally, Appellant notes that the "the name of the game is the claim." The Federal Circuit has held that claims must be interpreted both in light of the specification and in light of surrounding claims. With this in mind, note that when Appellant recites an intermediate key in terms of its relationship with the ultimate decryption of content, Appellant has carefully selected different words to distinguish one from the other. That is why Claim 44 refers to an intermediate key Kc that is used "to decrypt content streamed over the channel".

1033-130 APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 6

PATENT
Filed: January 8, 2002

signaling that while K_c is used in the decryption process it cannot be "useful in decrypting content" itself. That is, it is noteworthy that nowhere does Claim 44 recite that the key K_c itself "is useful for decrypting content", in contrast to the specifically direct recitation of the title key K_T in Claim 41 (and Claim 46, which both consistently and exclusively describe the title key as being "useful for decrypting content.") Indeed, when the claims are interpreted in light of the specification, this difference in claim language looms large, clearly distinguishing the claimed title key from the relied-upon program key P_k .

As a further reason to reverse, consider that the element in Richards relied on for the claimed "session key" - the channel access key CAK - does not appear to change (see, e.g., figures 18, 20, 21, and 22 and accompanying explanation in col. 12, explaining that S_k , P_k , and CC_k change, *but not the relied-upon CAK*.) This is important, because the term "session key" plainly implies a key that is unique to a session. While the examiner dismisses "session" as a mere "title" that safely can be ignored particularly since it is "not defined in the claim", rejections predicated on ignoring adjectives that are informed both by ordinary meaning and usage in the specification simply cannot be sustained. Left unexplained in the rejection is how "session" is being interpreted to read on a key CAK that apparently does not change, the evidentiary basis for that interpretation, and why one skilled in the art would accord the channel access key of Richards the meaning of a "session key."

Turning now to independent Claim 44, nowhere does Richards discuss that the relied-upon user encryption variable (UEV) is received upon registration. All that Richards states about the UEV are the three components that are combined to render it, col. 11, lines 1-10. Richards does not state when the components are received or combined, much less that anything occurs upon registration. Mere untaught possibilities are insufficient to defeat patentability. The rejection merits reversal.

1033-130.APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 7

PATENT
Filed: January 8, 2002

Additionally, nowhere does Richards support the allegation that its control channel key CCU is received in response to subscribing to a channel. That is a concept that is never mentioned in the relied-upon portions of Richards. Mere untaught possibilities are insufficient to defeat patentability. For this further reason, the rejection merits reversal.

While Claim 45 inherits the patentability of Claim 44, the rejection of it is based on another wave of the wand to conjure something out of Richards that isn't there, this time alleging that a session block is in Richards. Unless the examiner is interpreting "session block" to mean "anything", the rejection merits reversal. The concept of a block or matrix of keys simply is never mentioned in Richards.

(b) The examiner has been reminded that rejections should be strictly confined to the best available art. Cumulative rejections should be avoided, MPEP §706.02. The examiner has brushed aside the reminder. Appellant regrets the resulting inconvenience to the Board.

Of relevance to Claims 1 and 24 is the allegation that Ishigaro et al. obtains a channel unique key (relying on "e") by combining a channel key (relying on "e1") with a session key (relying on "e2"). Once again, the examiner is ignoring claim terms that have meaning. The relied-upon keys e1 and e2 are encrypted versions of session keys. Neither is said to be in any way uniquely related to a channel, nor has the examiner explained this discrepancy. The session keys appear to be generated in the DVD and thus function more like device keys, but in any event, Ishiguro et al. does not even mention the word "channel" anywhere in its text. The examiner is either making things up out of non-existent teachings of Ishiguro et al., or is writing the modifier "channel unique" out of the claim.

1053-130.APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 8

PATENT
Filed: January 8, 2002

Equally problematic is the superficiality with which the *prima facie* case has been made. Recall that Ishiguro et al. has been proposed to be combined with Yokota et al., but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered. Instead, the sole reason proffered for the proposed combination is that Ishiguro et al. "improves security of authentication and transmitted information by preventing an unauthorized user from posing as an authorized user", relying on paragraph 14 and figure 7.

First, paragraph 14 makes clear that what is being protected against is unauthorized use of an authorized device. That, however, has no relevance to Yokota et al. which seeks to protect content on a disk. Thus, the relied-upon suggestion in the secondary reference simply does not relate to the primary reference. There is lacking, in other words, a tie-in of the relied-upon suggestion to the primary reference. Since almost every patent extols its virtues in a vacuum, the fundamental *sine qua non* of patentability - the requisite prior art suggestion to combine - would be eviscerated should the present *prima facie* case be accorded legitimacy.

(c) Of relevance to Claims 1 and 24 is the allegation that Ishigaro et al. obtains a channel unique key (relying on "c") by combining a channel key (relying on "c1") with a session key (relying on "e2"). Once again, the examiner is ignoring claim terms that have meaning. The relied-upon keys e1 and e2 are encrypted versions of session keys. Neither is said to be in any way uniquely related to a channel, nor has the examiner explained this discrepancy. The session keys appear to be generated in the DVD and thus function more like device keys, but in any event, Ishiguro et al. does not even mention the word "channel" anywhere in its text. The examiner is either making things up out of non-existent teachings of Ishiguro et al., or is writing the modifier "channel unique" out of the claim.

1083 1.00 APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 9

PATENT
Filed: January 8, 2002

Equally problematic is the superficiality with which the *prima facie* case has been made. Recall that Ishiguro et al. has been proposed to be combined with Knauft, but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered. Instead, the sole reason proffered for the proposed combination is that Ishiguro et al. "improves security of authentication and transmitted information by preventing an unauthorized user from posing as an authorized user", relying on paragraph 14 and figure 7.

As paragraph 14 of the secondary reference makes clear, what is being protected against is unauthorized use of an authorized device. Knauft already deals with this problem - by providing the user key device in addition to the machine key device. Nowhere has any evidence of record been pointed to that Knauft recognizes a need for duplicate protection, or that either reference recognizes the interchangeability of user key devices of the primary reference with the relied-upon algorithm of the secondary reference. The rules for making a proper *prima facie* case of obviousness have once again not been complied with.

(d) Of relevance to Claims 1 and 24 is the allegation that Ishiguro et al. obtains a channel unique key (relying on "e") by combining a channel key (relying on "c1") with a session key (relying on "e2"). Once again, the examiner is ignoring claim terms that have meaning. The relied-upon keys e1 and e2 are encrypted versions of session keys. Neither is said to be in any way uniquely related to a channel, nor has the examiner explained this discrepancy. The session keys appear to be generated in the DVD and thus function more like device keys, but in any event, Ishiguro et al. does not even mention the word "channel" anywhere in its text. The examiner is either making things up out of non-existent teachings of Ishiguro et al., or is writing the modifier "channel unique" out of the claim.

1053-150.APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 10

PATENT
Filed: January 8, 2002

Equally problematic is the superficiality with which the *prima facie* case has been made. Recall that Ishiguro et al. has been proposed to be combined with Knauft, but no reference-specific analysis of why it would be obvious to combine the secondary reference with the very different primary reference has been offered. Instead, the sole reason proffered for the proposed combination is that Ishiguro et al. "improves security of authentication and transmitted information by preventing an unauthorized user from posing as an authorized user", relying on paragraph 14 and figure 7.

As paragraph 14 of the secondary reference makes clear, what is being protected against is unauthorized use of an authorized device. Nothing in the rejection explains that Richards recognizes that an unauthorized user might view Richards' TV, and Appellant can discern no suggestion of this in Richards. Nothing in the Office Action explains where the secondary reference suggests that its principles of prohibiting unauthorized use of its DVD player extends to a TV, and Appellant can discern no suggestion of this in Ishiguro et al. Thus, no evidence exists of record to motivate the skilled artisan to combine the DVD protection scheme of the secondary reference into the TV of Richards, a concept not recognized by either reference.

(e) For the reasons advanced above, it appears that the claims rejected under this subheading are patentable. Further, it does not appear that the device keys of Ishiguro et al. are used to activate the player, as otherwise recited in Claim 5, nor does anything resembling a key block, much less a session key block, appear in the secondary reference as otherwise recited in Claim 9, much less still the further delimiting steps of Claims 10-17.

1053-130 APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 11

PATENT
Filed: January 8, 2002

(f) For the reasons advanced above, it appears that the claims rejected under this subheading are patentable. Further, it does not appear that the device keys of Ishiguro et al. are used to activate the player, as otherwise recited in Claim 5, nor does anything resembling a key block, much less a session key block, appear in the secondary reference as otherwise recited in Claim 9, much less still the further delimiting steps of Claims 10-17.

(g) For the reasons advanced above, it appears that the claims rejected under this subheading are patentable. Further, it does not appear that the device keys of Ishiguro et al. are used to activate the player, as otherwise recited in Claim 5, nor does anything resembling a key block, much less a session key block, appear in the secondary reference as otherwise recited in Claim 9, much less still the further delimiting steps of Claims 10-17.

Respectfully submitted,


John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-130.APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 12

PATENT
Filed: January 8, 2002

APPENDIX A - APPEALED CLAIMS

1. A method for securely transmitting multicast data, comprising:
 1. encrypting at least one title T with at least title key K_T ; and
 2. encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{K_{cu}}(K_T)$, $S_{K_T}(T)$, wherein the channel-unique key K_{cu} is the result of a combination of a channel key K_c and a session key K_s .
3. The method of Claim 1, wherein the combination is a hash function of a concatenation of the channel key K_c and session key K_s .
4. The method of Claim 1, wherein the session key K_s is encrypted with at least a first encryption scheme B_{s1}^R to render a session key block.
5. The method of Claim 4, comprising providing at least one player with device keys K_d to activate the player.
6. The method of Claim 5, comprising providing the player with the channel key K_c .
7. The method of Claim 6, wherein at least one of the providing acts is undertaken in a point-to-point communication.

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 13

PATENT
Filed: January 8, 2002

8. The method of Claim 6, wherein at least one of the providing acts is undertaken as part of a broadcast.
9. The method of Claim 6, comprising providing the player with the session key block.
10. The method of Claim 9, wherein the player can determine the session key K_s from the session key block using the device keys K_d .
11. The method of Claim 10, comprising periodically refreshing the channel key K_c to enforce subscriptions.
12. The method of Claim 10, comprising selectively updating the session key block.
13. The method of Claim 12, comprising updating the session key block by encrypting an updated session key with at least the encryption scheme $B_{s,1}^R$.
14. The method of Claim 11, wherein a new channel key K_c' is encrypted with at least a second encryption scheme $B_{c,2}^R$.
15. The method of Claim 14, wherein the new channel key K_c' is sent in a message that is split.

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 14

PATENT
Filed: January 8, 2002

16. The method of Claim 14, wherein the new channel key K_c' is refreshed using plural messages.
17. The method of Claim 14, wherein the encryption scheme $B_{\mathcal{R}_2}^R$ includes:
assigning each player in a group of players respective private information L_u ;
partitioning players not in a revoked set R into disjoint subsets S_1, \dots, S_m having associated subset keys L_1, \dots, L_m ; and
encrypting the session key K_S with the subset keys L_1, \dots, L_m to render m encrypted versions of the session key K_S .
18. The method of Claim 17, wherein the encryption scheme $B_{\mathcal{R}_2}^R$ further includes partitioning the players into groups S_1, \dots, S_w , wherein "w" is an integer, and the groups establish subtrees in a tree.
19. The method of Claim 18, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i .
20. The method of Claim 19, wherein the revoked set R defines a spanning tree, and wherein the method includes:
initializing a cover tree T as the spanning tree;

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 15

PATENT
Filed: January 8, 2002

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

21. The method of Claim 19, wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each player is assigned labels from all nodes hanging from a direct path between the player and the root but not from nodes in the direct path.
22. The method of Claim 21, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.
23. The method of Claim 1, wherein the data is streamed to players.
24. A method for enforcing copy protection compliance and subscription compliance, comprising:
 - providing players with respective device keys K_d useful for enabling copy protection compliance;
 - providing players with at least one channel key K_c useful for enabling subscription compliance, such that a player can decrypt content only if the player is both compliant with copy protection and the player is an active subscriber to a content channel;
 - encrypting at least one title T with at least title key K_T ; and

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 16

PATENT
Filed: January 8, 2002

encrypting the title key K_T with at least one channel-unique key K_{cu} using at least one encryption function S to render a multicast data channel encrypted as $S_{K_{cu}}(K_T)$, $S_{KT}(T)$, wherein the channel-unique key K_{cu} is the result of a combination of the channel key K_c and a session key K_s .

25. The method of Claim 24, wherein the content is streamed to players.
28. The method of Claim 24, wherein the combination is a hash function of a concatenation of the channel key K_c and a session key K_s .
29. The method of Claim 24, wherein the session key K_s is encrypted with at least a first encryption scheme $B_{s,1}^R$ to render a session key block.
30. The method of Claim 29, comprising providing at least one player with its respective device keys K_d to activate the player.
31. The method of Claim 30, comprising providing the player with the channel key K_c upon or in response to subscription.
32. The method of Claim 30, wherein at least one of the providing acts is undertaken in a point-to-point communication.

1053-130.APP

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 17

PATENT
Filed: January 8, 2002

33. The method of Claim 30, wherein at least one of the providing acts is undertaken as part of a broadcast.
34. The method of Claim 30, comprising providing the player with the session key block.
35. The method of Claim 34, wherein the player can determine the session key K_c from the session key block using the device keys K_d .
36. The method of Claim 35, comprising periodically refreshing the channel key K_c to enforce subscriptions.
37. The method of Claim 34, comprising selectively updating the session key block.
38. The method of Claim 35, wherein the new channel key K_c' is refreshed by encrypting a new channel key K_c' with at least one encryption scheme.
39. The method of Claim 38, wherein the new channel key K_c' is sent in a message that is split.
40. The method of Claim 38, wherein the new channel key is refreshed using plural messages.
41. A player for decrypting streamed content, comprising:

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 18

PATENT
Filed: January 8, 2002

at least one device key K_d ;
means for decrypting a session key K_s using the device key K_d ;
means for decrypting a channel unique key K_{cu} using at least the session key K_s ; and
means for deriving a title key K_T using at least the channel unique key K_{cu} , the title key K_T
being useful for decrypting content.

42. The player of Claim 41, wherein the content is multicast to the player.

43. The player of Claim 42, wherein the player includes means for receiving streamed content,
and the content is streamed to the player.

44. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer,
comprising:

logic means for receiving private information I_u upon registration with a content provider;
logic means for subscribing to at least one content channel provided by the content provider;
logic means for receiving at least one encrypted channel key K_c at least partially in response
to subscribing to the channel;
logic means for deriving the channel key K_c using the information I_u ; and
logic means for using at least the channel key K_c to decrypt content streamed over the
channel.

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 19

PATENT
Filed: January 8, 2002

45. The computer program device of Claim 44, further comprising:
plural device keys K_d ;
logic means for receiving at least one session key block;
logic means for deriving at least one session key K_s from the session key block using at least one device key K_d .
46. The computer program device of Claim 45, further comprising:
logic means for using the session key K_s and channel key K_c to derive a channel unique key K_{cu} ; and
logic means for using the channel unique key K_{cu} to decrypt a title key K_t useful for decrypting the content.
47. The method of Claim 14, wherein the new channel key K_c' is sent in-band with the title T.
48. The method of Claim 38, wherein the new channel key K_c' is sent in-band with the title T.

FROM ROGITZ 619 338 8078

(THU) JAN 19 2006 16:37/ST. 16:33/No. 6833031675 P 21

CASE NO.: ARC920010090US1
Serial No.: 10/042,652
January 19, 2006
Page 20

PATENT
Filed: January 8, 2002

APPENDIX B - EVIDENCE

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

1053-130.ATT

CASE NO.: **ARC920010090US1**
Serial No.: **10/042,652**
January 19, 2006
Page 21

PATENT
Filed: January 8, 2002

APPENDIX C - RELATED PROCEEDINGS

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

1053-130.APP

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.